cited reference 3

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-134302
(43)Date of publication of application : 21.05.1999

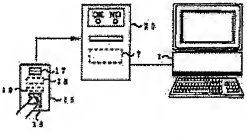
(51)Int.Cl. G06F 15/00
G06F 1/00
G06T 7/00
G06K 17/00
G06K 19/10

(21)Application number : 09-300176
(22)Date of filing : 31.10.1997

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : KUBO TAKEHIRO

(54) ACCESS CONTROLLER FOR TERMINAL, AND AUTHENTICATION CARD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent an authentication card from being used by an illegal user and to eliminate the need to change settings of readers connected to individual terminals even when users increase or decrease in number by sending terminal use permission information when a fingerprint of a user matches fingerprint information registered in an authentication device.
SOLUTION: The user after pressing his or her fingerprint against a card type authentication device 15 inserts the side wherein a terminal use information entry unit 17 is built into a card reader 20. The card reader 20 reads the terminal user permission information out of the terminal use information entry unit 17. A terminal use permission information decision unit 7 built in the card reader 20 decides whether or not the read information read by the card reader 20 is correct. When the information is correct, information for allowing the terminal 1 to be used to the terminal 1. The terminal 1 receives the information sent from the terminal user permission information decision unit 7 and allows the user to use the terminal 1.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－134302

(43)公開日　平成11年(1999)５月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ 15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｆ
1/00	３７０	1/00	３７０Ｅ
Ｇ０６Ｔ 7/00		Ｇ０６Ｋ 17/00	Ｖ
Ｇ０６Ｋ 17/00		Ｇ０６Ｆ 15/62	４６０
19/10		Ｇ０６Ｋ 19/00	Ｓ

審査請求　未請求　請求項の数12　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－300176

(22)出願日　平成９年(1997)10月31日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　久保　剛弘
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

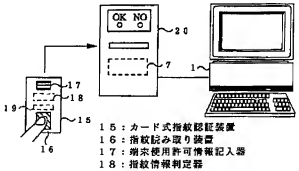
(74)代理人　弁理士　宮田　金雄　（外２名）

(54)【発明の名称】　端末のアクセス制御装置および認証カード

(57)【要約】

【課題】　従来のアクセス制御方式は、端末に利用者のパスワードを打ち込む方法や磁気カードや集積回路を組み込んだカードを使用する方法や、利用者の指紋を利用する方法を用いていた。しかし、パスワードを打ち込む方法や磁気カードや集積回路を組み込んだカードを使用する方法では、パスワードや磁気カード、集積回路を組み込んだカードを不正な利用者によって利用される可能性があった。一方、利用者の指紋を利用する方法では、利用者の増減によって端末に接続されている全ての指紋認証装置の設定を変更する必要があった。

【解決手段】　カード式認証装置に組み込まれた端末使用許可情報を、登録された指紋情報と利用者の指紋が一致した場合に書き込むことによって、不正な利用者が利用することを防ぎ、又、利用者の増減があった場合にも、個々の端末に接続された読み取り装置の設定を変更せずに済むようにする。



【特許請求の範囲】

【請求項1】　情報検索等を行う端末のアクセス制御装置において、カード読み取り装置に設けられ、端末使用許可情報を判定し、正しい情報であった場合、端末に使用許可情報を送信し、端末を使用可能にする端末使用許可情報判定器と、端末を使用しようとする際に、利用者自体の指紋と、予め登録してある指紋情報とが一致した場合に、端末使用許可情報を記録する認証カードと、上記認証カードに設けられ、利用者自体の指紋を読み取る指紋読み取り器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記認証カードに電気を供給する電源と、端末に接続され、利用者が端末を利用しようとする場合、利用者が所持している上記認証カードが挿入され、その端末使用許可情報を読み取り、端末使用許可情報判定器に送信するカード読み取り装置とを備えたことを特徴とする端末のアクセス制御装置。

【請求項2】　端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって、この認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、予め登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、複数の利用者の指紋情報が登録されたメモリとを備えたことを特徴とする認証カード。

【請求項3】　端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって上記認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記読み取った指紋情報と登録された利用者の指紋情報とが不一致の場合不正利用された事を報知する報知手段とを備えたことを特徴とする認証カード。

【請求項4】　上記報知手段はスピーカあるいは無線の送受信器で構成したことを特徴とする請求項3記載の認証カード。

【請求項5】　利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と予め登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、内部電源と、外部から供給された電気によって上記内部電源を充電する充電器とを備えたことを特徴とする認証カード。

【請求項6】　端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録するカード式認証装置と、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、内部電源と、内部電源に電気を供給する太陽電池とを備えたことを特徴とする認証カード。

【請求項7】　端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって上記認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、内部電源と、認証カードを振動させることで発電し、上記内部電源に電気を供給する振動発電器を備えたことを特徴とする認証カード。

【請求項8】　カード読み取り装置に設けられ、端末使用許可情報を判定し、正しい情報であった場合、端末に使用許可情報を送信し、端末を使用可能にする端末使用許可情報判定器と、端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードと、上記認証カードに設けられ、利用者自体の指紋を読み取る指紋読み取り器と、上記認証カードに設けられ、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記認証カードをカード読み取り装置に挿入した際、カード読み取り装置から電源を供給する外部電源器と、端末に接続され、利用者が所持している認証カードが挿入されたときその端末使用許可情報を読み取り、上記端末使用許可情報判定器に送信するカード読み取り装置と、上記カード読み取り装置に設けられ、認証カードが上記カード読み取り装置に挿入された際に電気を供給する電源供給器とを備えたことを特徴とする端末のアクセス制御装置。

【請求項9】　端末を使用しようとする際に、予め登録

してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって、上記認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、利用者の使用時間を登録し、その使用時間を過ぎた利用者については、上記端末使用許可情報記録器へ端末使用許可情報を記録するのを禁止するタイマーとを備えたことを特徴とする認証カード。

【請求項１０】　端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって、上記認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、利用者の使用回数を登録し、その使用回数を過ぎた利用者については、上記端末使用許可情報記録器へ端末使用許可情報を記録するのを禁止するカウンタとを備えたことを特徴とする認証カード。

【請求項１１】　カード読み取り装置に設けられ、端末使用許可情報を判定し、正しい情報であった場合、端末に使用許可情報を送信し、端末を使用可能にする端末使用許可情報判定器と、端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードと、上記認証カードに設けられ、利用者自体の指紋を読み取る指紋読み取り器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報を赤外線で送信する送信器と、上記赤外線で送信された端末使用許可情報を受信して、端末使用許可情報判定器に送信する受信器とを備えたことを特徴とする端末のアクセス制御装置。

【請求項１２】　カード読み取り装置に設けられ、端末使用許可情報を判定し、正しい情報であった場合、端末に使用許可情報を送信し、端末を使用可能にする端末使用許可情報判定器と、端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードと、上記認証カードに設けられ、利用者自体の指紋を読み取る指紋読み取り器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報を赤外線で送信する送信器と、上記赤外線で送信された端末使用許可情報を受信して、端末使用許可情報判定器に送信する受信器とを備えたことを特徴とする端末のアクセス制御装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は端末に接続し、端末を使用する際に、端末を使用する資格がない利用者であった場合、端末を使用できないようにする端末のアクセス制御装置および認証カードに関するものである。

【０００２】

【従来の技術】まず、従来における不正な利用者による端末の使用を制限する端末のアクセス制御について説明する。図１３において、１は端末であり、利用者は端末を利用して情報の検索等の作業を行う。２はキーボードであり、端末１に接続されている。３は利用者情報判定器であり、端末１に内蔵され、利用者がキーボード２から入力した情報から、その利用者が端末を使用する資格のある利用者であるかどうかを判定する。ここで利用者が端末１を使用する場合について説明する。利用者が端末１を使用する場合、利用者は端末１に接続されたキーボード２を使用して、登録された利用者名であるＬＯＧＩＮ名と、正しい利用者であることを示すための秘密情報であるＰＡＳＳＷＯＲＤを入力する。端末１に内蔵された利用者情報判定器３は、入力されたＬＯＧＩＮ名とＰＡＳＳＷＯＲＤが正しく登録されたものであるかを判定し、正しければ利用者に端末１の使用を許可する。

【０００３】しかし、ＬＯＧＩＮ名とＰＡＳＳＷＯＲＤは、不正な利用者によって知られた場合、端末が不正に使用される危険がある。また、利用者がＬＯＧＩＮ名やＰＡＳＳＷＯＲＤを忘れてしまった場合、端末を使用できなくなる可能性もある。そこで、図１４に示すような磁気カードを利用したり、図１５に示すような端末の利用許可情報が書き込まれた集積回路を組み込んだカードを利用したり、図１６に示すような指紋判定器を利用したりして、ＬＯＧＩＮ名とＰＡＳＳＷＯＲＤが、不正な利用者によって知られないようにしたり、又、ＬＯＧＩＮ名やＰＡＳＳＷＯＲＤを忘れてしまった場合、端末が使用できなくなるということを防いでいる。

【０００４】図１４は磁気カードを利用したアクセス制御を説明する図であって、図において４は磁気カードであり、端末１を利用する利用者が所持し、端末１を使用する場合に、端末１に接続されたカード読み取り装置６に挿入する。５は端末使用許可情報が書き込まれた磁気テープであり、磁気カード４に組み込まれていて、端末１の使用を許可するための情報が書き込まれている。６はカード読み取り装置であり、端末に接続され、利用者が端末１を利用しようとする場合、利用者が所持している磁気カード４を挿入し、磁気カード４に組み込まれ

た、端末使用許可情報が書き込まれた磁気テープ５から端末使用許可情報を読み取る。７は端末使用許可情報判定器であり、カード読み取り装置６に内蔵され、カード読み取り装置６が読み取った、磁気カード４の端末使用許可情報を判定し、情報が正しかった場合、端末１の使用を許可するための情報を端末１に送信する。

【０００５】次に動作について説明する。まず、利用者が端末１を使用する場合、所持している磁気カード４の端末使用許可情報が書き込まれた磁気テープ５が組み込まれた側をカード読み取り装置６に挿入する。カード読み取り装置６は、磁気カード４に組み込まれた端末使用許可情報が書き込まれた磁気テープ５から、端末使用許可情報を読み取る。カード読み取り装置６が、読み取った端末使用許可情報を、カード読み取り装置６に内蔵された端末使用許可情報判定器７が正しい情報であるかどうか判定し、正しい情報であれば、端末１の使用を許可するための情報を端末１に送信する。端末１はカード読み取り装置６に内蔵された端末使用許可情報判定器７から送信された使用を許可するための情報を受信し、利用者に対して端末を使用可能にする。カード読み取り装置６が読み取った情報が正しい情報でなかった場合には、端末使用許可情報判定器７は端末１の使用を許可するための情報を端末１に送信しない。従って、端末１は使用可能にならないため、利用者は使用することができない。

【０００６】図１５は集積回路を組み込んだカードを利用したアクセス制御を説明する図であって、図において７は図１４と同じである。８は集積回路を組み込んだカードであり、端末１を利用する利用者が所持し、端末１を使用する場合に、端末１に接続されたカード読み取り装置１０に挿入する。９は端末使用許可情報が書き込まれた集積回路であり、集積回路を組み込んだカード８に組み込まれていて、端末１の使用を許可するための情報が書き込まれている。１０はカード読み取り装置であり、端末１に接続され、利用者が端末１を利用しようとする場合、利用者が所持している集積回路を組み込んだカード８を挿入し、集積回路を組み込んだカード８に組み込まれた、端末使用許可情報が書き込まれた集積回路９から端末使用許可情報を読み取る。

【０００７】次に動作について説明する。まず、利用者が端末１を使用する場合、所持している集積回路を組み込んだカード８の端末使用許可情報が書き込まれた集積回路９が組み込まれた側をカード読み取り装置１０に挿入する。カード読み取り装置１０は、集積回路を組み込んだカード８に組み込まれた端末使用許可情報が書き込まれた集積回路９から、端末使用許可情報を読み取る。カード読み取り装置１０が、読み取った端末使用許可情報を、カード読み取り装置１０に内蔵された端末使用許可情報判定器７が正しい情報であるかどうか判定し、正しい情報であれば、端末１の使用を許可するための情報を端末１に送信する。端末１はカード読み取り装置１０に内蔵された端末使用許可情報判定器７から送信された使用を許可するための情報を受信し、利用者に対して端末を使用可能にする。カード読み取り装置１０が読み取った情報が正しい情報でなかった場合には、端末使用許可情報判定器７は端末１の使用を許可するための情報を端末１に送信しない。従って、端末１は使用可能にならないため、利用者は使用することができない。

【０００８】図１６は指紋認証装置を利用したアクセス制御を説明する図であって、図において１１は指紋認証装置であり、端末１に接続され、利用者が端末１を使用する場合に、利用者が指紋を押し付ける。１２は指紋読み取り器であり、指紋認証装置１２に組み込まれていて、利用者が押し付けた指紋を読み取る。１３は指紋判定器であり、指紋読み取り器１２が読み取った利用者の指紋情報と複数の指紋の情報を記憶するメモリ１４に記憶された指紋の情報が一致するかどうかを判定し、一致した場合、端末１の使用を許可するための情報を端末１に送信する。１４は複数の指紋の情報を記憶するメモリであって、端末１を使用できる複数の利用者の指紋の情報が記憶されている。

【０００９】次に動作について説明する。まず、利用者が端末１を使用する場合、利用者の指紋を、指紋認証装置１１に組み込まれた指紋読み取り器１２に押し付ける。指紋読み取り器１２は、押し付けられた利用者の指紋の情報を読み取る。指紋読み取り器１２が読み取った利用者の指紋の情報を、指紋認証装置１１に内蔵された指紋判定器１３が、同じく指紋認証装置１１に内蔵された複数の指紋の情報を記憶するメモリ１４に記憶された、端末の使用を許可する利用者の指紋の情報と比較する。指紋判定器１３は、指紋読み取り器１２が読み取った指紋の情報が複数の指紋の情報を記憶するメモリ１４に記憶された指紋の情報と一致した場合、端末１の使用を許可するための情報を端末１に送信する。端末１は指紋認証装置１１から送信された使用を許可するための情報を受信し、利用者に対して端末を使用可能にする。一方、指紋読み取り器１２が読み取った指紋の情報が複数の指紋の情報を記憶するメモリ１４に記憶された指紋の情報と一致しなかった場合には、指紋判定器１３は端末１の使用を許可するための情報を端末１に送信しない。従って、端末１は使用可能にならないため、利用者は使用することができない。

【００１０】

【発明が解決しようとする課題】従来の端末のアクセス制御装置は、上記のように端末の使用を制限していた。しかし、磁気カードや集積回路を組み込んだカードによってアクセス制御を行う方法では、磁気カードや集積回路を組み込んだカードを利用者が紛失し、不正な利用者によって使用される可能性があった。一方、利用者の指紋を利用してアクセス制御を行う方法では、利用者が増

えたり、減ったり、あるいは変更があった場合、端末に接続された全ての指紋認証装置の設定を変更する必要がある。端末の台数が少ない場合は、変更作業も容易だが、端末の台数が増えた場合は、変更作業は繁雑になる。

【0011】この発明は上記のような問題点を解消するためになされたもので、利用者の指紋とカード式の認証装置に登録された指紋情報が一致した場合に、端末使用許可情報を記入することで、不正な利用者が利用することを防ぎ、又、利用者の増減があった場合にも、個々の端末に接続された読み取り装置の設定を変更せずに済むようにすることを目的とする。

【0012】

【課題を解決するための手段】第1の発明による端末のアクセス制御装置は、利用者の指紋を認識し、正しい利用者であった場合に、端末使用許可情報記入器に、端末使用許可情報を記入し、その情報をカード読み取り装置が読み取るようにすることで、カード式認証装置が不正な利用者の手に渡った場合でも、不正な利用者が端末を利用できないようにする。

【0013】第2の発明による認証カードは、複数の指紋の情報を記憶するためのメモリを備えることで、複数の利用者が同じ認証カードを利用できるようにする。

【0014】第3の発明による認証カードは、認証カードが不正な利用者に使用されている場合、不正な利用者が端末を使用できないだけでなく、端末が不正に使用されようとしているという事実を離れた場所に知らせることができるようにする。

【0015】第4の発明による認証カードは、認証カードが不正な利用者に使用されている場合、無線で通信又は音を出すことによって、不正な利用者が端末を使用できないだけでなく、端末が不正に使用されようとしているという事実を周囲に知らせることができるようにする。

【0016】第5の発明による認証カードは、外部電源から電気を供給できるようにすることで、内部電源に充電できるようにする。

【0017】第6の発明による認証カードは、太陽電池を使用することで、太陽電池の部分に光が当たれば、内部電源に電気を供給できるようにする。

【0018】第7の発明による認証カードは、振動により発電する発電器を備えることで、認証カードを振動させれば、内部電源に電気を供給できるようにする。

【0019】第8の発明による端末のアクセス制御装置は、カード読み取り装置から電気の供給を受けることができるようにすることで、内部電源がなくても認証カードが利用できるようにする。

【0020】第9の発明による認証カードは、使用時間を記憶するタイマーを備えることで、利用者の使用時間が過ぎた場合、認証カードが使用できないようにする。

【0021】第10の発明による認証カードは、使用回数を記憶するカウンターを備えることで、利用者の使用回数が過ぎた場合、認証カードが使用できないようにする。

【0022】第11の発明による端末のアクセス制御装置は、利用者の指紋を認識し、正しい利用者であった場合に、端末使用許可情報を無線を使用して送信することで、端末から離れた場所から、利用者が正しい利用者かどうかを認証することができるようにする。

【0023】第12の発明による端末のアクセス制御装置は、利用者の指紋を認識し、正しい利用者であった場合に、端末使用許可情報を赤外線を使用して送信することで、端末から離れた場所から、利用者が正しい利用者かどうかを認証することができるようにする。

【0024】

【発明の実施の形態】

実施の形態1．図1は、この発明の実施の形態1を示す図であり、図において1、7は図15と同じである。15はカード式認証装置（認証カード）であって、端末1を使用する利用者は、指紋を押し付けて、カード読み取り装置20に挿入する。16は指紋読み取り器であって、カード式認証装置15に組み込まれていて、利用者が押し付けた指紋を読み取る。17は端末使用許可情報記入器であって、カード式認証装置15に組み込まれており、指紋読み取り器16が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを指紋情報判定器18が判定し、一致した場合に端末使用許可情報が書き込まれる。18は指紋情報判定器であって、カード式認証装置15に内蔵されており、登録してある指紋情報と、指紋読み取り器16が読み取った利用者の指紋情報とが一致するかどうかを判定し、一致した場合には、端末使用許可情報記入器17に端末使用許可情報を書き込む。19は内部電源であって、カード式認証装置15に電気を供給する。20はカード読み取り装置であり、端末1に接続され、利用者が端末1を利用しようとする場合、利用者が所持しているカード式認証装置15を挿入し、カード式認証装置15に組み込まれた、端末使用許可情報記入器17から端末使用許可情報を読み取る。

【0025】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置15の持ち主である利用者が端末1を使用する場合、利用者はカード式認証装置15に組み込まれている指紋読み取り器16に自分の指紋を押し付ける。指紋読み取り器16は利用者の指紋を読み取り、カード式認証装置15に内蔵されている指紋情報判定器18に読み取った情報を送る。指紋情報判定器18は送られた情報が登録されている指紋情報と一致するかを判定する。この場合は、カード式認証装置15の持ち主である利用者であるため、送られた情報と登録されている指

紋情報は一致し、カード式認証装置１５に組み込まれている端末使用許可情報記入器１７に端末使用許可情報が書き込まれる。指紋読み取り器１６、端末使用情報記入器１７、指紋情報判定器１８は、それぞれ、カード式認証装置１５に内蔵された内部電源１９から電気を供給されている。

【００２６】利用者は自分の指紋をカード式認証装置１５に押し付けた後、カード読み取り装置２０に、端末使用情報記入器１７が組み込まれた側を挿入する。カード読み取り装置２０は、端末使用情報記入器１７から端末使用許可情報を読み取る。カード読み取り装置２０が、読み取った情報を、カード読み取り装置２０に内蔵された端末使用許可情報判定器７が正しい情報であるかどうかを判定する。この場合は正しい情報であるので、端末１の使用を許可するための情報を端末１に送信する。端末１は端末使用許可情報判定器７から送信された使用を許可するための情報を受信し、利用者に対して端末を使用可能にする。

【００２７】次に、カード式認証装置１５の持ち主でない利用者がカード式認証装置１５を使用した場合、指紋読み取り器１６は利用者の指紋を読み取り、カード式認証装置１５に内蔵されている指紋情報判定器１８に読み取った情報を送る。この場合は、カード式認証装置１５の持ち主でないため、送られた情報と登録されている指紋情報は一致せず、カード式認証装置１５に組み込まれている端末使用許可情報記入器１７に端末使用許可情報が書き込まれない。その後、利用者はカード読み取り装置２０に、端末使用情報記入器１８が組み込まれた側を挿入する。カード読み取り装置２０は、端末使用情報記入器１８から端末使用許可情報を読み取る。カード読み取り装置２０が、読み取った情報を、カード読み取り装置２０に内蔵された端末使用許可情報判定器７が正しい情報であるかどうかを判定する。この場合は正しくない情報であるので、端末１の使用を許可するための情報は端末１に送信されず、利用者は端末を使用することができない。このようにして、カード式認証装置の持ち主以外の利用者が、端末を使用するのを防ぐことを可能にする。

【００２８】実施の形態２．図２は、この発明の実施の形態２を示す図であり、図において１５～１９は図１と同じである。２１は複数の指紋情報を記憶するメモリであって、カード式認証装置１５に内蔵されており、複数の利用者の指紋情報を記憶している。

【００２９】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置１５の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置１５に組み込まれている指紋読み取り器１６に自分の指紋を押し付ける。指紋読み取り器１６は利用者の指紋を読み取り、カード式認証装置１５に内蔵されている指紋情報判定器１８に読み取った情報を送る。指紋情報判定器１８は送られた情報がカード式認証装置１５に内蔵されている複数の指紋の情報を記憶するメモリ２１に登録されている複数の指紋情報のうち一つと一致するかを判定する。この場合は、カード式認証装置１５の持ち主である利用者であるため、送られた情報と登録されている指紋情報は一致し、指紋情報判定器１８は端末使用許可情報記入器１７に端末使用許可情報を書き込む。このようにして、複数の利用者が同じカード式認証装置を使用することを可能にする。

【００３０】また、カード式認証装置１５の持ち主である他の利用者が、情報検索等の作業を行うために端末の使用する場合、利用者はカード式認証装置１５に組み込まれている指紋読み取り器１６に自分の指紋を押し付ける。指紋読み取り器１６は利用者の指紋を読み取り、カード式認証装置１５に内蔵されている指紋情報判定器１８に読み取った情報を送る。指紋情報判定器１８は送られた情報がカード式認証装置１５に内蔵されている複数の指紋の情報を記憶するメモリ２１に登録されている複数の指紋情報のうちの一つと一致するかを判定する。この場合は、カード式認証装置１５の持ち主である利用者であるため、送られた情報と登録されている指紋情報は一致し、指紋情報判定器１８は端末使用許可情報記入器１７に端末使用許可情報を書き込む。このようにして、複数の利用者が同じカード式認証装置を使用することを可能にする。

【００３１】実施の形態３．図３は、この発明の実施の形態３を示す図であり、図において１５～１９は図１と同じである。２２は不正利用された事を無線で送信する無線通信器であって、カード式認証装置１５に組み込まれており、指紋読み取り器１６が読み取った利用者の指紋情報が、指紋情報判定器１８に登録された利用者の指紋情報と一致しなかった場合、正規の利用者でない人物が端末を使用しようとしているという情報を無線で送信する。２３は無線通信器からの情報を受信する受信器であって、不正利用された事を無線で送信する無線通信器２２から、正規の利用者でない人物がカード式認証装置１５を使用しようとしているという情報を無線で受信する。

【００３２】次に動作について説明する。例えば、カード式認証装置１５の持ち主でない利用者が端末を使用しようとする場合、利用者はカード式認証装置１５に組み込まれている指紋読み取り器１６に自分の指紋を押し付ける。指紋読み取り器１６は利用者の指紋を読み取り、カード式認証装置１５に内蔵されている指紋情報判定器１８に読み取った情報を送る。指紋情報判定器１８は送られた情報と登録されている指紋情報とが一致するかを判定する。この場合は、カード式認証装置１５の持ち主

でない利用者であるため、送られた情報と登録されている指紋情報は一致しない。従って、指紋情報判定器18は、カード式認証装置15に組み込まれている不正利用された事を無線で送信する無線通信器22に、正規の利用者でない利用者がカード式認証装置15を使用しているという情報を送る。不正利用された事を無線で送信する無線通信器22は、受信した情報を無線で送信する。無線通信器からの情報を受信する受信器23は、カード式認証装置15に組み込まれた無線通信器22から、正規の利用者でない利用者がカード式認証装置15を使用しているという情報を受信する。指紋読み取り器16、端末使用情報記入器17、指紋情報判定器18、不正利用された事を無線で送信する無線通信器22は、それぞれ、カード式認証装置15に内蔵された内部電源19から電気を供給されている。このようにして、正規の利用者でない人物が端末を使用しようとしているという情報を、離れた場所で知ることを可能にする。

【0033】実施の形態4．図4は、この発明の実施の形態4を示す図であり、図において15～19は図1と同じである。24は不正利用された事を音で知らせるスピーカーであって、カード式認証装置15に組み込まれており、指紋読み取り器16が読み取った利用者の指紋情報が、指紋情報判定器18に登録された利用者の指紋情報と一致しなかった場合、正規の利用者でない人物がカード式認証装置15を使用しようとしているという情報を音で周りに知らせる。

【0034】次に動作について説明する。例えば、カード式認証装置15の持ち主でない利用者が端末を使用しようとする場合、利用者はカード式認証装置15に組み込まれている指紋読み取り器16に自分の指紋を押し付ける。指紋読み取り器16は利用者の指紋を読み取り、カード式認証装置15に内蔵されている指紋情報判定器18に読み取った情報を送る。指紋情報判定器18は送られた情報と登録されている指紋情報とが一致するかを判定する。この場合は、カード式認証装置15の持ち主でない利用者であるため、送られた情報と登録されている指紋情報は一致しない。従って、指紋情報判定器18は、カード式認証装置15に組み込まれている不正利用された事を音で知らせるスピーカー24に、正規の利用者でない利用者がカード式認証装置15を利用しているという信号を送る。不正利用された事を音で知らせるスピーカー24は、受信した信号によって、音を発生し、正規の利用者でない利用者がカード式認証装置15を使用しているということを周囲に知らせる。指紋読み取り器16、端末使用情報記入器17、指紋情報判定器18、不正利用された事を音で知らせるスピーカー24は、それぞれ、カード式認証装置15に内蔵された内部電源19から電気を供給されている。このようにして、正規の利用者でない人物が端末を使用しようとしているという情報を、周囲の人間が知ることを可能にする。

【0035】実施の形態5．図5は、この発明の実施の形態5を示す図であり、図において15～19は図1と同じである。25は外部から供給された電気によって内部電源を充電する充電器であって、カード式認証装置15に内蔵されており、外部から電気を供給する電源装置26から、電気を供給を受けて内部電源19の充電を行う。26は外部から電気を供給する電源装置であって、外部から供給された電気によって内部電源を充電する充電器25に電気を供給する。

【0036】次に動作について説明する。例えば、カード式認証装置15に内蔵された内部電源19の電気が残り少なくなり、指紋読み取り器16、端末使用情報記入器17、指紋情報判定器18が機能しなくなった際、外部から電気を供給する電源装置26を使用して、外部から供給された電気によって内部電源を充電する充電器25に電気を供給する。外部から供給された電気によって内部電源を充電する充電器25は供給された電気を、カード式認証装置15に内蔵された内部電源19に電気を供給する。内部電源19に電気が供給されることで、指紋読み取り器16、端末使用情報記入器17、指紋情報判定器18を再び機能させることが可能になる。このようにして、内部電源の電気が少なくなっても、外部から供給することで、再びカード式認証装置を利用可能にする。

【0037】実施の形態6．図6は、この発明の実施の形態6を示す図であり、図において15～19は図1と同じである。27は太陽電池であって、カード式認証装置15に組み込まれており、外部からの光によって発電を行い、内部電源19に電気を供給する。

【0038】次に動作について説明する。例えば、カード式認証装置15に光を当てることによって、カード式認証装置15に組み込まれた太陽電池27が発電し、カード式認証装置15に内蔵された内部電源19に電気を供給する。このようにして、光を当てることで、カード式認証装置に電気を供給することを可能にする。

【0039】実施の形態7．図7は、この発明の実施の形態7を示す図であり、図において15～19は図1と同じである。28は振動によって発電する振動発電器であって、カード式認証装置15に内蔵されており、カード式認証装置15を振動させることによって発電を行い、内部電源19に電気を供給する。

【0040】次に動作について説明する。例えば、カード式認証装置15を振動させることによって、カード式認証装置15に組み込まれた振動によって発電する振動発電器28が発電し、カード式認証装置15に内蔵された内部電源19に電気を供給する。このようにして、振動させることによって、カード式認証装置に電気を供給することを可能にする。

【0041】実施の形態8．図8は、この発明の実施の形態8を示す図であり、図において7、15～18、2

０は図１と同じである。２９はカード読み取り装置から電源を供給する外部電源器であって、カード式認証装置１５に組み込まれており、カード認証装置１５がカード読み取り装置２０に挿入された時に、カード読み取り装置２０に内蔵された電源供給器３０から電気を供給される。３０は電源供給器であって、カード読み取り装置２０に組み込まれており、カード式認証装置１５が挿入された時に、カード式認証装置１５に電気を供給する。

【００４２】次に動作について説明する。例えば、カード式認証装置１５の利用者がカード式認証装置１５に組み込まれた指紋読み取り器１６に指紋を押し付けたまま、カード式認証装置１５をカード読み取り装置２０に挿入する。カード読み取り装置２０に組み込まれた電源供給器３０は、カード式認証装置１５が挿入された際、カード式認証装置１５に組み込まれたカード読み取り装置２０から電源を供給する外部電源器２９に電気を供給する。電気を供給されたカード読み取り装置２０から電源１を供給する外部電源器２９は、指紋読み取り器１６、端末使用情報記入器１７、指紋情報判定器１８に電気を供給する。このことにより、指紋読み取り器１６が利用者の指紋を読み取り、指紋情報判定器１８が正しい利用者の指紋情報であるかを判断し、端末使用情報記入器１７に端末使用許可情報を書き込む。端末使用情報記入器１７に書き込まれた端末使用許可情報をカード読み取り装置２０が読み取り、カード読み取り装置２０に内蔵された端末使用許可情報判定器７が正しい情報であるかどうかを判定する。正しい情報であった場合、カード読み取り装置２０に内蔵された端末使用許可情報判定器７は、端末の使用を許可する情報を端末に送信し、利用者は端末を使用することができる。このようにして、カード式認証装置本体に電源がなくても、カード式認証装置を利用可能にする。

【００４３】実施の形態９．図９は、この発明の実施の形態９を示す図であり、図において１５～１９は図１と同じである。３１は使用時間を記憶するタイマーであって、カード式認証装置１５に内蔵されており、使用時間を記憶し、予め登録された使用時間が過ぎた場合、端末使用許可情報記入器１７に、端末使用許可情報が書き込めないようにする。

【００４４】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置１５の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置１５に組み込まれている指紋読み取り器１６に自分の指紋を押し付ける。指紋読み取り器１６は利用者の指紋を読み取り、カード式認証装置１５に内蔵されている指紋情報判定器１８に読み取った情報を送る。指紋情報判定器１８は送られた情報と登録されている指紋情報と一致するかを判定する。同時に、使用時間を記憶するタイマー３１が、カード式認証装置１５の使用時間をチェックする。利用者の使用時間が使用時間を記憶するタイマー３１に記憶された使用時間を過ぎていた場合、カード式認証装置１５に組み込まれている端末使用許可情報記入器１７に端末使用許可情報が書き込めないようにする。この場合、利用者の指紋と登録されている指紋情報は一致しても、カード式認証装置１５は使用できない。このようにして、カード式認証装置の使用時間を決めておき、使用時間を過ぎた利用者がカード式認証装置を利用することを不可能にする。

【００４５】実施の形態１０．図１０は、この発明の実施の形態１０を示す図であり、図において１５～１９は図１と同じである。３２は使用回数をカウントするカウンタであって、カード式認証装置１６に内蔵されており、使用回数をカウントし、予め登録された使用回数が過ぎた場合、端末使用許可情報記入器１７に、端末使用許可情報が書き込めないようにする。

【００４６】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置１５の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置１５に組み込まれている指紋読み取り器１６に自分の指紋を押し付ける。指紋読み取り器１６は利用者の指紋を読み取り、カード式認証装置１５に内蔵されている指紋情報判定器１８に読み取った情報を送る。指紋情報判定器１８は送られた情報と登録されている指紋情報と一致するかを判定する。同時に、使用回数をカウントするカウンタ３２が、カード式認証装置１５の使用回数のカウントを行い、予め登録された使用回数とのチェックを行う。利用者の使用回数が使用回数をカウントするカウンタ３２に記憶された使用回数を過ぎていた場合、カード式認証装置１５に組み込まれている端末使用許可情報記入器１７に端末使用許可情報が書き込めないようにする。この場合、利用者の指紋と登録されている指紋情報は一致しても、カード式認証装置１５は使用できない。このようにして、カード式認証装置の使用回数を決めておき、使用回数を過ぎた利用者がカード式認証装置を利用することを不可能にする。

【００４７】実施の形態１１．図１１は、この発明の実施の形態１１を示す図であり、図において７、１５、１６、１８、１９は図１と同じである。３３は端末使用許可情報を無線で送信する無線通信器であって、カード式認証装置１５に内蔵されており、端末使用許可情報を無線で送信する。３４は端末使用許可情報を無線で受信する受信器であって、端末使用許可情報を受信する。

【００４８】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置１５の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置１５に組み込まれている指紋読み取り器１６に自分の指紋を押し付ける。指紋読み取り器１６は利用者の指紋を読み取り、カード

式認証装置１５に内蔵されている指紋情報判定器１８に読み取った情報を送る。指紋情報判定器１８は送られた情報と登録されている指紋情報とが一致するかを判定し、一致した場合、端末使用許可情報をカード式認証装置１５に組み込まれている端末使用許可情報を無線で送信する無線通信器２２に送信する。端末使用許可情報を無線で送信する無線通信器３２は、指紋情報判定器１８から送られた端末使用許可情報を、端末に接続されている端末使用許可情報を無線で受信する受信器３４に無線で送信する。端末使用許可情報を無線で受信する受信器３４は、端末使用許可情報を受信すると、端末使用許可情報を無線で受信する受信器３４に内蔵された端末使用許可情報判定器７に情報を送る。端末使用許可情報を無線で受信する受信器３４に内蔵された端末使用許可情報判定器７は、受信した情報が正しい情報であるかどうかを判定し、正しい情報であった場合、端末に使用許可情報を送信する。このようにして、端末から離れた場所から、カード式認証装置を利用して端末を使用することを可能にする。

【００４９】実施の形態１２．図１２は、この発明の実施の形態１２を示す図であり、図において７、１５、１６、１８、１９は図１と同じである。３５は端末使用許可情報を赤外線で送信する送信器であって、カード式認証装置１５に内蔵されており、端末使用許可情報を赤外線で送信する。３６は端末使用許可情報を赤外線で受信する受信器であって、端末使用許可情報を受信する。

【００５０】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置１５の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置１５に組み込まれている指紋読み取り器１６に自分の指紋を押し付ける。指紋読み取り器１６は利用者の指紋を読み取り、カード式認証装置１５に内蔵されている指紋情報判定器１８に読み取った情報を送る。指紋情報判定器１８は送られた情報と登録されている指紋情報とが一致するかを判定し、一致した場合、端末使用許可情報をカード式認証装置１５に組み込まれている端末使用許可情報と赤外線で送信する送信器３５に送信する。端末使用許可情報を赤外線で送信する送信器３５は、指紋情報判定器１８から送られた端末使用許可情報を、端末に接続されている端末使用許可情報を赤外線で受信する受信器３６に赤外線で送信する。端末使用許可情報を無線で受信する受信器３４は、端末使用許可情報を受信すると、端末使用許可情報を赤外線で受信する受信器３６に内蔵された端末使用許可情報判定器７に情報を送る。端末使用許可情報を赤外線で受信する受信器３６に内蔵された端末使用許可情報判定器７は、受信した情報が正しい情報であるかどうかを判定し、正しい情報であった場合、端末に使用許可情報を送信する。このようにして、端末から離れた場所から、カード式認証装置を利用して端末を使用することを可能にする。

【００５１】

【発明の効果】第１の発明によれば、認証カードに、利用者自体の指紋を読取り、読取られた指紋と登録してある指紋情報が一致した場合、端末の使用許可情報を書き込むことで、認証カードの持ち主以外の利用者が、端末を使用するのを防ぐことができる。

【００５２】第２の発明によれば、認証カードに複数の利用者の指紋情報を登録することのできるメモリを内蔵することで、複数の利用者が認証カードを使用することができる。

【００５３】第３の発明によれば、認証カードの持ち主でない利用者が、端末を使用しようとしていることを、報知することで、離れた場所で認証カードの持ち主でない人物が、端末を使用しようとしているということを知ることができる。

【００５４】第４の発明によれば、認証カードの持ち主でない利用者が、端末を使用しようとしているということを、無線又は音を出して知らせることで、周囲に認証カードの持ち主でない人物が、端末を使用しようとしているということを知らせることができる。

【００５５】第５の発明によれば、認証カードが充電することを可能にすることで、内部電源の電気容量が少なくなっても、充電することにより、内部電源の電気容量を回復することができる。

【００５６】第６の発明によれば、認証カードに太陽電池を組み込むことで、光を当てることで発電し、認証カードを利用することができる。

【００５７】第７の発明によれば、認証カードに振動によって発電する発電器を備えることで、振動によって発電し、認証カードを利用することができる。

【００５８】第８の発明によれば、認証カードがカード読み取り装置から電気を供給するようにすることで、認証カードに電源を持たなくても、認証カードを利用することができる。

【００５９】第９の発明によれば、認証カードに使用時間を登録することで、その使用時間を過ぎた認証カードの利用者が、認証カードを使用できないようにすることができる。

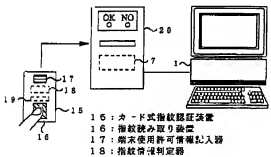
【００６０】第１０の発明によれば、認証カードに使用回数を登録することで、その使用回数を過ぎた認証カードの利用者が、認証カードを使用できないようにすることができる。

【００６１】第１１の発明によれば、端末使用許可情報を無線で送信することで、端末から離れた場所から、認証カードを利用して端末を使用することを可能にする。

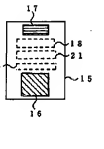
【００６２】第１２の発明によれば、端末使用許可情報を赤外線で送信することで、端末から離れた場所から、認証カードを利用して端末を使用することを可能にする。

【図面の簡単な説明】
【図1】　この発明の実施の形態1を示す図である。
【図2】　この発明の実施の形態2を示す図である。
【図3】　この発明の実施の形態3を示す図である。
【図4】　この発明の実施の形態4を示す図である。
【図5】　この発明の実施の形態5を示す図である。
【図6】　この発明の実施の形態6を示す図である。
【図7】　この発明の実施の形態7を示す図である。
【図8】　この発明の実施の形態8を示す図である。
【図9】　この発明の実施の形態9を示す図である。
【図10】　この発明の実施の形態10を示す図である。
【図11】　この発明の実施の形態11を示す図である。
【図12】　この発明の実施の形態12を示す図である。
【図13】　従来の端末におけるアクセス制御を示す図である。
【図14】　磁気カードを使用した従来のアクセス制御を示す図である。
【図15】　集積回路を組み込んだカードを使用した従来のアクセス制御を示す図である。
【図16】　指紋読み取り装置を使用した従来のアクセス制御を示す図である。
【符号の説明】
1　端末、2　キーボード、3　利用者情報判定器、4　磁気カード、5　磁気テープ、6　カード読み取り装置、7　端末使用許可情報判定器、8　カード、9　集積回路、10　カード読み取り装置、11　指紋認証装置、12　指紋読み取り器、13　指紋判定器、14　メモリ、15　カード式指紋認証装置、16　指紋読み取り装置、17　端末使用許可情報記入器、18　指紋情報判定器、19　内部電源、20　カード読み取り装置、21　メモリ、22　無線通信器、23　受信器、24　スピーカー、25　充電器、26　電源装置、27太陽電池、28　振動発電器、29　外部電源器、30　電源供給器、31タイマー、32　カウンタ、33　無線通信器、34　受信器、35　送信器、36　受信器。

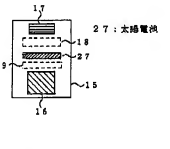
【図1】



【図2】

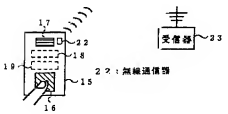


【図6】

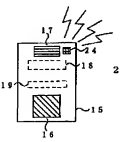


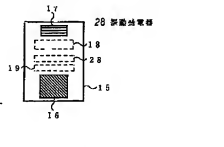
【図7】

【図3】



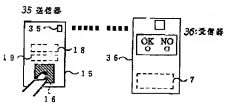
【図4】

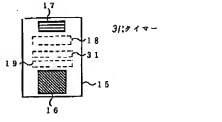




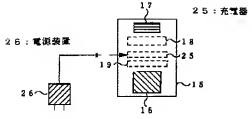
【図9】

【図12】

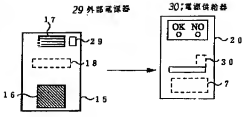




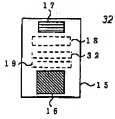
【図5】



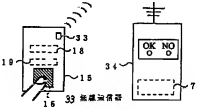
【図8】



【図10】

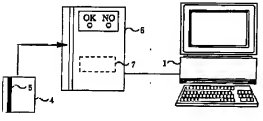


【図11】

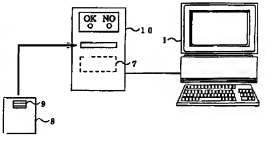


【図13】

【図14】



【図15】



【図16】